EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 10116029
PUBLICATION DATE : 06-05-98

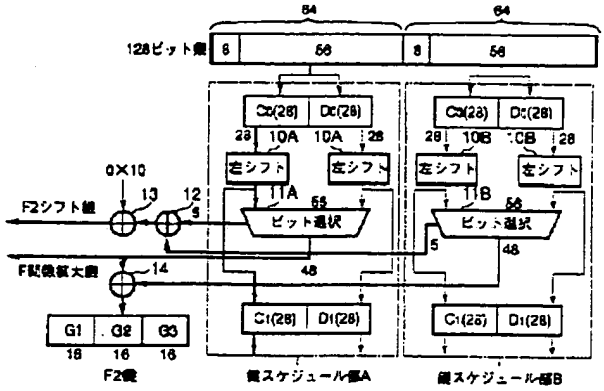
APPLICATION DATE : 11-10-96
APPLICATION NUMBER : 08269897

APPLICANT : TOSHIBA CORP;

INVENTOR : SAKURAI KOICHI;

INT.CL. : G09C 1/00

TITLE : CIPHERING DEVICE AND ITS METHOD



ABSTRACT : PROBLEM TO BE SOLVED: To provide a ciphering device capable of increasing safety while compatibility with DES(data encryption standard) is maintained.

SOLUTION: This device is provided with two identically structured key schedule parts A, B for developing two ciphering keys, which are obtainable by bisecting key information consisting of prescribed bit lines, each into an intermediary key for stirring an inputted message; with an exclusive OR part 14 for determining an exclusive OR against the two intermediary keys outputted from these two key schedule parts A, B; and with a stirring part for stirring the inputted message, using one of the intermediary keys if the two keys are detected being identical to each other with the exclusive OR turning zero, and using both keys if the two keys compared are detected being unidentical to each other.

COPYRIGHT: (C) JPO

Best Available Copy

H04 L 9/06

Pour le titre du livre
voir en seconde page

IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, May 9-10, 1991

XP 000280289

An Expanded Set of Design Criteria for Substitution Boxes and Their Use in Strengthening DES-like Cryptosystems

Michael H. Dawson and Stafford E. Tavares

Department of Electrical Engineering
Queen's University
Kingston, Ontario, K7L 3N6

p. 191 - 195 = (5)

Abstract — The security of DES-like cryptosystems depends heavily on the strength of the Substitution boxes (S-boxes) used. The design of new S-boxes is therefore an important concern in the creation of new and more secure cryptosystems. The full set of design criteria for the S-boxes of DES has never been released and a complete set has yet to be proposed in the open literature. This paper introduces a unified S-box design framework based on information theory and illustrates how it can be used to strengthen and design the S-boxes used in DES-like cryptosystems.

Introduction

DES-like cryptographic algorithms are based on substitution-permutation networks (SP networks). In these cryptosystems encryption is carried out using alternating layers of substitutions and permutations as shown in Figure 1. In this class of cryptosystem the security depends heavily on the properties of the substitution (S-boxes) which are used. Since it is very difficult to create large S-boxes with known properties they are often built out of smaller S-boxes as shown in Figure 2. Unfortunately this construction does not produce the best possible S-boxes and increases the importance of the properties of the smaller S-boxes used. It is therefore very important to use S-boxes with the best possible properties in the construction of DES-like cryptosystems.

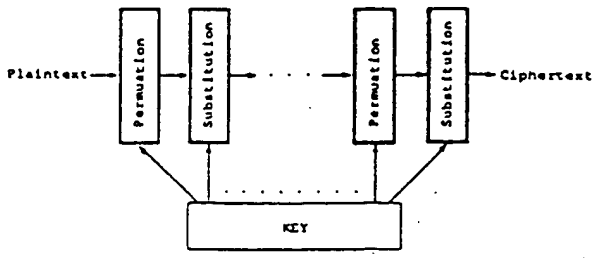


Figure 1 Substitution-Permutation Network

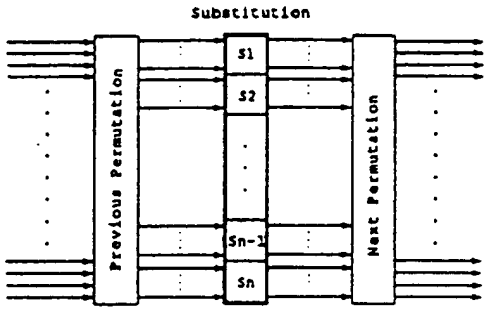


Figure 2 Use of a set of smaller Substitutions to create a larger one

In this paper we present a unified S-box design framework based on information theoretic concepts and we show that by using these criteria we can find S-boxes which can be used to build stronger cryptosystems. As an example we illustrate how strengthened S-boxes can be easily integrated into the DES structure. The criteria are also used to explain some aspects of the construction of the DES S-boxes.

Background

Cryptographic substitutions, first introduced by Shannon in [1], were further refined and explained in [2][3]. It has been shown in [4][5] and more recently in [6] that poor S-boxes can lead to weak cryptosystems. The S-boxes of DES [7] have been subject to much analysis (see [8][9][10][11] and others).

Work on defining desirable properties of S-boxes has been presented in [12][13][14][15][16][17]. More recently, some properties based on information theory were presented by Forré in [11]. Despite the previous investigations into the desirable properties of S-boxes, a comprehensive set of design criteria for S-boxes has yet to be presented.

We will extend the set of desirable properties of S-boxes using information theory and use these properties to propose a set of design criteria for S-boxes.

Static and Dynamic Views of an S-box

S-boxes can be viewed in two ways. The first is the static view of the S-box which describes the S-box when the inputs are

CH2954-6/91-0000-191 $1.00 © 1991 IEEE

BNSDOCID: <XP 280289A >

not changing. The second is the dynamic view of the S-box which describes the S-box when the inputs are changing.

Much of the previous work on S-boxes has focussed on the static properties of S-boxes. The static view of an S-box, with inputs $X = [x_1, ..., x_m]$ and outputs $Y = [y_1, ..., y_n]$, can be envisioned as shown in Figure 3.

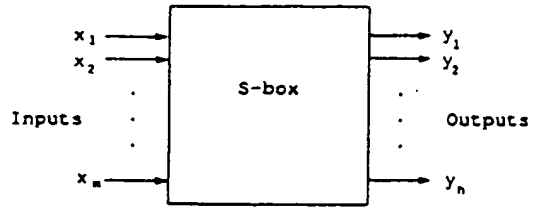


Figure 3 Static View of an m×n S-box

The importance of certain dynamic properties of an S-box were introduced by Feistel in [2] and refined in [14]. More recently Biham and Shamir's work on differential cryptanalysis[6] stimulated us to discover that a broader range of dynamic properties of S-boxes are important in DES-like cryptosystems. When considering the dynamic properties of an S-box, it is useful to refer to the delta S-box shown in Figure 4.

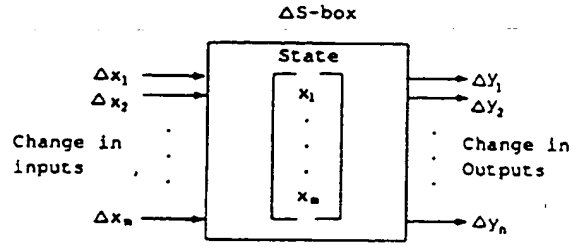


Figure 4 Dynamic View of an m×n S-box

In Figure 4 the values of the vector $X = [x_1, ..., x_m]$ are the current inputs to the S-box and can be viewed as the state of the delta S-Box. The Δx_i and the Δy_i are the changes in the inputs and outputs respectively. The current state X is usually unknown and it is assumed that any relation found between the Δx_i and the Δy_i is over all possible states.

Properties of Ideal S-boxes Based on Information Theory

An "Ideal" S-box should behave as randomly as possible; however, due to the deterministic nature of S-boxes, the input-output relations are known. The best an Ideal S-box can do then, is to behave as randomly as possible when only partial information is known about the inputs and outputs. In [11] Forré developed two properties of an Ideal m×n bit S-box based on similar ideas. Her first property was that the uncertainty in the output bits is not reduced by the knowledge of any subset of the input bits. The second property was that the uncertainty in any unknown output bits is not reduced by the knowledge of the other output bits.

We have defined a set of six properties that an Ideal S-box must meet. This set of properties has a broader scope than those of Forré and any S-box that meets these properties will also meet Forré's. The properties are grouped into a set of static properties and a set of dynamic properties.

Static Properties

The first static property is that partial information about the inputs and outputs of an S-box does not reduce the uncertainty in an unknown output. Note that this is a stronger property than Forré's because partial knowledge about the output is also given. More formally:

$$H(y_i \mid x_{j_1}, ..., x_{j_k}, y_{l_1}, ..., y_{l_s}) = H(y_i)$$

for all $i, k, l, s, p \mid 1 \le i \le n, 1 \le k \le m-1, 1 \le j_1, ..., j_k \le m, 1 \le s \le n-1, 1 \le (l_1, ..., l_s, p) \le n, l_p \ne i$.

The second static property is that partial information about the inputs and outputs does not reduce the uncertainty in an unknown input. This property is required because the S-box can often be attacked from both the input and output directions. Note that this is a stronger property than Forré's because partial knowledge about the input is also given. More formally:

$$H(x_i \mid x_{j_1}, ..., x_{j_k}, y_{l_1}, ..., y_{l_s}) = H(x_i)$$

for all $i, k, l, s, p \mid 1 \le i \le m, 1 \le k \le m-1, 1 \le (j_1, ..., j_k, p) \le m, 1 \le s \le n-1, 1 \le l_1, ..., l_s \le n, j_p \ne i$.

The third static property is that the uncertainty in a data value is reduced by the minimum amount possible when it passes through an S-box. This means that uncertainty in the output of the S-box is as great as the uncertainty in the input of the S-box, and if this is not possible, because $m > n$, that the uncertainty in the output is the maximum for the number of output bits. This property is desirable so that one cannot guess the output of the S-box more easily that the input. More formally, let $X = [x_1, ..., x_m]$, $Y = [y_1, ..., y_n]$ where $m \ge n$, then :

$$H(Y) = \begin{cases} H(X), & \text{if } H(X) \le n \\ n, & \text{if } H(X) > n \end{cases}$$

BNSDOCID: <XP____280289A__1_>

Dynamic Properties

The dynamic properties are similar to the static properties except that they deal with the changes to the inputs and outputs. The dynamic properties are defined in the same way as the corresponding static properties except the inputs and outputs are replaced by the changes in the inputs and outputs. For example the first dynamic property is that partial information about the changes in the inputs and outputs does not reduce the uncertainty in changes of the unknown outputs is defined formally as:

$$H(\Delta y_i \mid \Delta x_{j_1}, ..., \Delta x_{j_k}, \Delta y_{l_1}, ..., \Delta y_{l_s}) = H(\Delta y_i)$$

for all $i, k, l, s, p \mid 1 \leq i \leq n, 1 \leq j_1, ..., j_k, k \leq m, 1 \leq s \leq n-1, 1 \leq (l_1, ..., l_s, p) \leq n, l_p \neq i$. It is assumed that the state of the delta S-box is unknown and any properties hold over all states.

Design Criteria

Using the information theoretic properties of an Ideal S-box we define a set of static and dynamic criteria for m×n bit S-boxes. The definitions of the static properties refer to the static S-box and are for an m×n bit S-box with inputs X and outputs Y. There are 6 static properties: Input-Output Independence, Output-Input independence, Output-Output Independence, Non-linearity, Information Completeness, and Invertibility. The definitions of the dynamic properties refer to the delta S-box with changes to the inputs ΔX and changes to the outputs ΔY. There are 3 dynamic properties : Dynamic Input-Output Independence, Dynamic Output-Input Independence, and Output-Output Independence. In addition to the 9 information theoretic design criteria which are fundamental to any good S-box, we will discuss three types of avalanche criteria which may be necessary depending on how the S-boxes will be used.

The *Input-output Independence* criterion of order r is used to select S-boxes for which knowledge of r input values does not reduce the uncertainty in the output values. Formally an S-box meets the Input-output Independence criterion of order r, r < m, iff:

$$Prob(y_j \mid a_1 x_1, ..., a_m x_m) = Prob(y_j)$$

for all $x_i, y_j, a_k \mid 1 \leq j \leq n, 1 \leq i, k \leq m, (a_k, x_i, y_j) \in \{0,1\}, \sum_{k=1}^{m} a_k = r$ where $a_k = 1$ denotes that x_k is given and $a_k = 0$ denotes that x_k is not given. Note that the highest order of Input-output Independence that can be met is m-1. To meet Input-output Independence of order m the input-output relation would have to be unknown and this is never true.

The *Output-input Independence* criterion is used to select S-boxes for which knowledge of some of the outputs does not reduce the uncertainty in the inputs. This criterion is defined in exactly the same way as Input-output Independence except that the inputs and outputs are reversed.

The *Output-output Independence* criterion is used to select S-boxes for which partial information about the outputs bits does not reduce the uncertainty in the unknown output bits. Formally an S-box meets the Output-output Independence criterion of order r, r < n, iff:

$$Prob(y_j \mid a_1 y_1, ..., a_n y_n) = Prob(y_j)$$

for all $y_j, a_k \mid 1 \leq j, k \leq n, (a_k, y_j) \in \{0,1\}, a_j = 0, \sum_{k=1}^{n} a_k = r$ where $a_k = 1$ denotes that x_k is given and $a_k = 0$ denotes that x_k is not given. It is important to note that this criterion is met, for all orders of n-1 or less, by any invertible S-box because all of the 2^n possible outputs occur with equal probability assuming the inputs occur with equal probability. It can also be shown that any m×n bit S-box made up of invertible n×n bit S-boxes meets the Output-output Independence criterion for all orders up to m-1.

Non-linearity is a crucial property of an Ideal S-box. It is the Non-linearity of an S-box that prevents it from being expressed as a set of linear equations, which could then be used to break any cryptosystem using that S-box. Non-linearity has been proposed as a design criterion previously and is defined in [12].

Kam and Davida in [13] define Completeness as: for every possible input value every output bit depends on all input bits and not just a proper subset of the input bits. As noted by Forré in [11] this is a weak concept. We extend this definition, to define *Information Completeness*, by requiring that each output bit depend on all the Information in each input bit as opposed to depending on only part of the information in each bit.

The *Invertibility* criterion is generally known to be a desirable property of n×n S-boxes. An S-box is invertible iff it is a one to one mapping. More formally, an n bit S-box, S, is invertible iff,

$$S(X_1) = S(X_2) \;\; iff \;\; X_1 = X_2$$
$$\forall \{X_1, X_2 \in \{0,1\}^n\}$$

An Ideal n×n S-box must meet this criterion because otherwise there are fewer output values than there are input values. If there are fewer output values than input values there is less uncertainty in the output than in the input, and the third static property of an Ideal S-box will not be met.

The *Dynamic Input-output Independence* criterion, of order r, is used to select S-boxes for which knowledge of the changes in r inputs bits, does not reduce the uncertainty in the changes of the outputs. Formally, an S-box meets the Dynamic Input-output Independence criterion of order r, r <= m iff:

$$Prob(\Delta y_j \mid a_1 \Delta x_1, ..., a_m \Delta x_m) = Prob(\Delta y_j)$$

for all $\Delta x_i, \Delta y_j, a_k \mid 1 \leq j \leq n, 1 \leq i, k \leq m, (a_k, \Delta x_i, \Delta y_j) \in \{0,1\}, \sum_{k=0}^{m} a_k = r$ where $a_k = 1$ denotes that Δx_k is given and $a_k = 0$ denotes that Δx_k is not given. It can be shown that the Strict Avalanche Criterion introduced and defined in [14], and all its extensions, are a subset of Dynamic Input-output Independence of order m.

The *Dynamic Output-input Independence* criterion is used to select S-boxes for which knowledge of some of the output changes does not reduce the uncertainty in the input changes. This criterion is defined in exactly the same way as Dynamic Input-output Independence except that the input changes and output changes are reversed.

BNSDOCID: <XP____280269A__!_>

The *Dynamic Output-output Independence* criterion, of order r, is used to select S-boxes for which the knowledge of r of the output changes and a particular pattern of input changes, does not reduce the uncertainty in the unknown output bits. Formally an S-box meets the Dynamic Output-output Independence criterion of order r, r < n-1, iff:

$$Prob(\Delta y_j \mid a_1\Delta y_1, ..., a_n\Delta y_n, \Delta x_1, ..., \Delta x_m) = Prob(\Delta y_j \mid \Delta x_1, ..., \Delta x_m)$$

for all $\Delta x_i, \Delta y_j, a_k \mid 1 \leq j \leq n, 1 \leq i,k \leq m, (a_k, \Delta x_i, \Delta y_j) \in \{0,1\}, a_j = 0, \sum_{k=0}^{n} a_k = r$ where $a_k = 1$ denotes that Δx_k is given and $a_k = 0$ denotes that Δx_k is not given.

Many of the previously proposed design criteria for S-boxes are used to ensure that the cryptosystem in which they are used possesses certain kinds of avalanche. We do not view the properties which these criteria require as fundamental properties of S-boxes, however they may be necessary when S-boxes are used in certain types of cryptosystems. The avalanche properties can be divided into three classes: Probabilistic Avalanche, Directed Avalanche, and Minimal Avalanche. *Probabilistic Avalanche* criteria require that each output of an S-box change with probability 1/2 whenever the input is changed. The changes in the outputs must also be independent. All S-boxes which meet the dynamic information theoretic criteria will posses Probabilistic Avalanche and this is regarded as the only type of avalanche which is a fundamental property of a good S-box. *Directed Avalanche* criteria require that each output of an S-box change with probability 1/2 whenever certain patterns of change are made in the input. Again, the changes in the output bits must be independent. Examples of Directed Avalanche criteria are the Strict Avalanche Criterion (SAC) and all of its extensions. *Minimal Avalanche* criteria require that a minimum number of output bits changes when certain patterns of change are made in the input. The DES design criteria that requires that at least two output bits change when one input is changed is a good example of a Minimal Avalanche criterion. Neither Minimal nor Directed avalanche properties are fundamental to good S-boxes, however they may be useful whenever smaller S-boxes are used to create the larger substitutions required in SP network based cryptosystems. When smaller S-boxes are used in SP network based cryptosystems, the permutations used ensure that the outputs of individual S-boxes are distributed to the inputs of distinct S-boxes in the next round. This distribution has the effect of forcing certain patterns of changes in the input (those where 1 or 2 bits change) to be the most likely to occur in the early rounds. Due to this effect it is justified to used Minimal or Directed avalanche criteria to ensure that adequate avalanche will occur for those patterns of change. In other cryptosystems where all of the patterns of change in the inputs are equally likely it does not make sense to require Minimal or Directed Avalanche.

A more detailed description of the design framework can be found in [18, 19, 20]

Analysis of DES S-boxes Using The Design Criteria

We investigated both the properties of the DES 6×4 bit S-boxes and the DES 4×4 S-boxes. The investigations revealed that we could not find S-boxes with substantially better information theoretic properties than the S-boxes of DES and which also met the acknowledged DES design criteria. This indicates that the S-boxes of DES may be some of the best possible based on a combination of our information theoretic properties and the acknowledged DES design criteria. It is important to note that there were many S-boxes found which met the acknowledged DES design criteria but had poor information theoretic properties.

It was also revealed that the properties of the inverses of the DES 4×4 S-boxes were as good as those of the S-boxes themselves. This indicates that the designers of DES placed an equal emphasis on the properties of the S-boxes and their inverses.

In every case we found that the properties of the complete 6×4 S-boxes were better than any individual 4×4 sub-box. We concluded that using multiple sub-boxes to form a larger S-box is an important method that can be used to create S-boxes that have better properties than are possible in a single sub-box. This gives a possible explanation for why multiple sub-boxes were used to create the S-boxes of DES. Some of the unexplained DES design criteria may have been included to ensure that the properties of the S-boxes created from the 4×4 S-boxes were acceptable.

Further details of the investigations into the properties of the S-boxes of DES are contained in [19]

Applications of the Design Criteria

The design criteria can be used to create larger S-boxes for use in new cryptosystems. As previously discussed, larger S-boxes have better properties and therefore properly designed cryptosystems which use larger S-boxes should be stronger than those which use smaller S-boxes. The design criteria can also be used to select which S-boxes of a particular size should be used to create the best cryptosystems. Further details on the results of using the design criteria to create new and larger S-boxes is given in [19, 20]. The design criteria can also be used to strengthen current cryptosystems by allowing the currently used S-boxes to be evaluated and replaced with stronger ones if necessary. As an example we will discuss a possible approach that could be used to strengthen DES. Our investigations revealed that it was not possible to find 6×4 bit S-boxes with substantially better properties than those of the S-boxes of DES. We therefore suggest that 8×4 bit S-boxes formed from 16 4×4 bit S-boxes can be used. The larger S-boxes should have better properties because more S-boxes are combined together. Investigations of some sample 8×4 bit S-boxes revealed that they did posses better information theoretic properties than any of the DES 6×4 bit S-boxes. The integration of the larger S-boxes into DES is straightforward but will require a modified E expansion and key scheduling algorithm. A new E expansion is shown in Figure 5. The key scheduling algorithm must be modified so that there are two 32 bit halves and each half is shifted by 2 bits in each round. The use of larger halves requires the new PC-1 and PC-2 permutations which are shown in Figures 6 and 7. A discussion on the rules and methods used to create new expansions and permuted choices appears in [21].

BNSDOCID: <XP 2802994 >

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

DES E-BIT SELECTION TABLE

31	32	1	2	3	4	5	6
3	4	5	6	7	8	9	10
7	8	9	10	11	12	13	14
11	12	13	14	15	16	17	18
15	16	17	18	19	20	21	22
19	20	21	22	23	24	25	26
23	24	25	26	27	28	29	30
27	28	29	30	31	32	1	2

EXTENDED E-BIT SELECTION TABLE

Figure 5 Extended E Expansion

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

DES PC-1

57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	28	18	12	4
64	56	48	40	32	24	16	8
63	55	47	39	31	23	15	7
62	54	46	38	30	22	14	6
61	53	45	37	29	21	13	5

NEW PC-1

Figure 6 New PC-1

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	50	36	29	32

DES PC-2

1	6	11	16	21	26	31	15
2	7	12	17	22	27	32	20
3	8	13	18	23	28	5	25
4	9	14	19	24	29	10	30
33	38	43	48	53	58	63	47
34	39	44	49	54	59	64	52
35	40	45	50	55	60	37	57
36	41	46	51	56	61	42	62

NEW PC-2

Figure 7 New PC-2

The use of the larger S-boxes and the modified key scheduling algorithm increases the key size to a true 64 bits. The new permutations and expansions given are simple extensions of those used in DES. It should be emphasized that this is not a proposal for a strengthened DES but simply an illustration of an approach made possible by the use of our new design framework. The use of stronger S-boxes is seen as a key factor of any approach used to strengthen DES and increase its key size. The S-boxes determine the strength of the cryptosystem and increasing the key size without strengthening the S-boxes is not deemed to be wise.

Conclusions

In this paper we introduced the static and dynamic views of an S-box and used these abstractions to define the properties of an Ideal S-box based on information theoretic ideas. We then presented a new set of design criteria for S-boxes based on the properties of an Ideal S-box and illustrated how it can be used to strengthen DES-like cryptosystems. The new set of design criteria should be a valuable tool that can be used to create S-boxes for cryptosystems of the future.

Bibliography

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.

[2] H. Feistel, "Cryptography and computer privacy," *Scientific American*, vol. 228, no. 5, pp. 15–23, 1973.

[3] H. Feistel, W. Notz, and J. L. Smith, "Some cryptographic techniques for machine-to-machine data communications," in *Proceedins of the IEEE*, vol. 63, pp. 1545–1554, 1975.

[4] B. den Boer, "Cryptanalysis of F. E. A. L.," in *Advances in Cryptology: Proc. of EUROCRYPT 88*, pp. 167–173, Springer-Verlag, 1989.

[5] W. Fumy, "On the F-function of FEAL," in *Advances in Cryptology:Proc. of CRYPTO 87*, pp. 434–437, Springer-Verlag, 1988.

[6] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," in *Advances in Cryptology: Proc. of CRYPTO 90*, pp. 1–19, August, 1990.

[7] National Bureau of Standards (U.S.), "Data Encryption Standard (DES)," Tech. Rep. Publication 46, Federal Information Processing Standards, 1977.

[8] M. E. Hellman and et. al., "Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard," tech. rep., Information Systems Laboratory, Stanford University, November, 1976.

[9] A. Shamir, "On the security of DES," in *Advances in Cryptology: Proc. of CRYPTO 85*, pp. 280–281, Springer-Verlag, 1986.

[10] E. F. Brickell, J. H. Moore, and M. R. Purtill, "Structure in the S-boxes of the DES(extended abstract)," in *Advances in Cryptology: Proc. of CRYPTO 86*, pp. 3–8, Springer-Verlag, 1986.

[11] R. Forré, "Methods and instruments for designing S-boxes," *Journal of Cryptology*, vol. 2, no. 3, pp. 115–130, 1990.

[12] J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," in *IEE proceedings, Part E: Computers and Digital Techniques*, vol. 135, pp. 325–335, 1988.

[13] J. B. Kam and G. I. Davida, "Structured design of substitution-permutation encryption networks," *IEEE Transactions on Computers*, vol. C-28, pp. 747–753, 1979.

[14] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology:Proc. of CRYPTO 85*, pp. 523–534, Springer-Verlag, 1985.

[15] B. Preneel, W. VanLeewijck, L. VanLinden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of boolean functions," in *EUROCRYPT 90 — Abstracts*, pp. 155–165, 1990.

[16] S. Lloyd, "Properties of binary functions," in *EUROCRYPT 90 — Abstracts*, pp. 126–135, 1990.

[17] C. Adams and S. Tavares, "The structured design of cryptographically good S-boxes," *Journal of Cryptology*, vol. 3, pp. 27–41, 1990.

[18] M. Dawson and S. Tavares, "An expanded set of S-box design criteria and their relation to differential-like attacks," tech. rep., Queens University, Dec. 1990.

[19] M. Dawson, "A unified framework for Substitution box design based on information theory," Master's thesis, Queens University, 1991(to appear).

[20] M. Dawson and S. Tavares, "An expanded set of S-box design criteria and their relation to differential-like attacks," in *Advances in Cryptology: Proc. of EUROCRYPT 91*, p. to appear, 1991.

[21] L. Brown, "Analysis of the DES and its implications for the design of an extended DES," tech. rep., University of New South Wales, Dec. 1988.

BNSDOCID: <XP____280289A__I_>

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.